

EFFICIENT RANDOM NUMBER GENERATION FOR
COMMUNICATION SYSTEMS

ABSTRACT OF THE DISCLOSURE

5 Truly random numbers are generated with a minimum of extra hardware by taking
advantage of the inherent noise in a communication channel. Random numbers can thus
be generated without specialized manufacturing requirements and can be incorporated to
conventional integrated circuits with minimal additional logic. The random number
generation technique offloads the processor from performing extensive generation
10 calculations without the use of the hardware accelerator. This random number generation
technique may find application in, e.g., any network device that participates in a virtual
private network or is used to implement electronic commerce.